AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A computing device comprising:

a host processor coupled to a bus to execute a pre-operating system software program and an operating system present software program;

a non-volatile memory coupled to the host processor, the non-volatile memory to store ~~a~~ the pre-operating system software program;

a disk memory coupled to the bus, the disk memory to store ~~an~~ the operating system present software program and an operating system; and

a protected storage medium ~~configured~~ coupled to the host processor, the protected storage medium to enable secure exchange of a protected message between the pre-operating system software program and the operating system present software program.

2. (Original) The computing device of claim 1 further comprising:

a first interface to provide the pre-operating system software program access to the protected storage medium; and

a second interface to provide the operating system present software program access to the protected storage medium.

3. (Original) The computing device of claim 1 wherein the protected storage medium is a non-volatile re-writeable memory device.

4. (Cancelled).

5. (Previously Presented) The computing device of claim 1 wherein the protected message is exchanged during boot-up of the computing device.

6. (Cancelled).

7. (Previously Presented) The computing device of claim 1 wherein the protected message includes user authentication information.

8. (Cancelled).

9. (Previously Presented) The computing device of claim 1 wherein the protected storage medium is further configured to enable the operating system present software program to securely store the protected message for the pre-operating system software program subsequent to boot-up of the computing device.

10. (Currently Amended) The computing device of claim 9 wherein the protected message is retrieved by the pre-operating system software program during reboot of the computing device.

11. (Currently Amended) A method comprising:

~~providing a first interface to a protected storage medium to enable a~~ accessing, by a host processor executed pre-operating system software program, ~~access to~~ a protected storage medium;

~~enabling~~ performing, by the pre-operating system software program, ~~to perform secure storage of~~ a boot-up procedure according to a protected message ~~for~~ stored within the protected, storage medium by an operating system present software program ~~within the protected storage medium~~; and

~~providing a second interface to~~ storing, by the pre-operating system software program, boot-up information within the protected storage medium ~~to enable~~ for the operating system present software program according to ~~access the protected storage medium to enable secure exchange of~~ the protected message ~~between the pre-operating system software program and the operating system present software program~~.

12. (Currently Amended) The method of claim 11 wherein the ~~protected message includes user authentication information.~~storing comprises:

formatting user authentication information obtained during the boot-up procedure according to the protected message; and

securely storing the formatted user authentication information within the protected storage medium.

13. (Cancelled).

14. (Cancelled).

15. (Currently Amended) The method of claim 11 wherein ~~providing~~ accessing comprises:

detecting the protected message within protected storage medium;

~~enabling~~ performing, by the pre-operating system ~~present~~ software program, ~~to perform secure retrieval~~ an authentication procedure of the protected message from the protected storage medium; and

discarding the protected message if the authentication procedure fails.

16. (Currently Amended) The method of claim ~~15~~ 11 wherein the ~~protected message is stored during~~ storing the boot-up ~~of the computing device.~~ information comprises:

encrypting the boot-up information; and

wrapping the encrypted boot-up information within a digital signature of the pre-operating system program.

17. (Cancelled).

18. (Previously Presented) The method of claim 11 further comprising:

enabling the operating system present software program to perform secure storage of a protected request for the pre-operating system software program subsequent to boot-up of the computing device.

19. (Previously Presented) The method of claim 18 wherein enabling comprises:

enabling the pre-operating system software program to perform secure retrieval of the protected request from the protected storage medium.

20. (Previously Presented) The method of claim 19 wherein the protected request is retrieved by the pre-operating system software program during reboot of the computing device.

21. (Currently Amended) A machine readable medium having instructions stored thereon which when executed by a processor cause the processor to perform operations comprising:

~~providing a first interface to a protected storage medium to enable a~~ accessing, by a host processor executed pre-operating system software program, ~~access to a~~ protected storage medium;

~~enabling~~ performing, by the pre-operating system software program, ~~to perform secure storage of~~ a boot-up procedure according to a protected message ~~for~~ stored within the protected, storage medium by an operating system present software program ~~within the protected storage medium~~; and

~~providing a second interface to~~ storing, by the pre-operating system software program, boot-up information within the protected storage medium ~~to enable~~for the operating system present software program according to ~~access the protected storage medium to enable secure exchange of~~ the protected message ~~between the pre-operating system software program and the operating system present software program~~.

22. (Cancelled).

23. (Cancelled).

24. (Currently Amended) The machine readable medium of claim 21 wherein the ~~instructions~~ accessing the protected storage medium causes the processor to perform further operations comprising:

detecting the protected message within protected storage medium;

~~enabling~~ performing, by the pre-operating system ~~present~~ software program, ~~to perform secure retrieval~~ an authentication procedure of the protected message from the protected storage medium; and

discarding the protected message if the authentication procedure fails.

25. (Previously Presented) The machine readable medium of claim 21 wherein the instructions cause the processor to perform further operations comprising:

enabling the operating system present software program to perform secure storage of a protected request for the pre-operating system software program subsequent to boot-up of the device.

26. (Previously Presented) The machine readable medium of claim 21 wherein the instructions cause the processor to perform further operations comprising:

enabling the pre-operating system software program to perform secure retrieval of the information from the protected storage medium during reboot of the computing device.

27. (Currently Amended) The method of claim 11 further comprising:

accessing, ~~via the second interface~~by an operating system present user authentication software program, user authentication information from the protected storage; and

authenticating, by ~~an~~ the operating system present user authentication software program, a user according to the user authentication information.

28. (Currently Amended) The method of claim 11, wherein ~~providing~~ performing further comprises:

requesting, by a pre-operating system user authentication software program, user authentication information according to the protected message;

accessing~~, via the first interface,~~ user ~~authentication~~ verification information from the protected storage;

authenticating, by ~~an~~ the pre-operating system ~~present~~ user authentication software program, a user according to the user authentication information and the user verification information; and

~~storing , via the second interface, user authentication information from the protected storage, if the user authentication is successful; and~~

~~otherwise,~~ disabling boot-up of a computing device if the user authentication is unsuccessful.

29. (Currently Amended) The machine readable medium of claim 21 wherein the instructions cause the processor to perform further operations comprising:

accessing, ~~via the second interface~~by an operating system present user authentication software program, user authentication information from the protected storage; and

authenticating, by ~~an~~ the operating system present user authentication software program, a user according to the user authentication information.

30. (Currently Amended) The machine readable medium of claim 21, wherein ~~the instructions~~ performing causes the processor to perform further operations comprising:

requesting, by a pre-operating system user authentication software program, user authentication information according to the protected message;

accessing~~, via the first interface,~~ user ~~authentication~~ verification information from the protected storage;

authenticating, by an operating system present user authentication software program, a user according to the user authentication information and the user verification information; and

~~storing , via the second interface, user authentication information from the protected storage, if the user authentication is successful; and~~

~~otherwise,~~ disabling boot-up of a computing device if the user authentication is unsuccessful.

Please add the following new claims:

--31. (New) The machine readable medium of claim 21, wherein storing causes the processor to perform further operations, comprising:

formatting user authentication information obtained during the boot-up procedure according to the protected message; and

securely storing the formatted user authentication information within the protected storage medium.

32. (New) The machine readable medium of claim 21, wherein storing causes the processor to perform further operations, comprising:

encrypting the boot-up information; and

wrapping the encrypted boot-up information within a digital signature of the pre-operating system program. --